Adventures in Algebraic Path Problems with applications to Internet routing SBRC Tutorial May 2019, Gramado, Brazil

Timothy G. Griffin

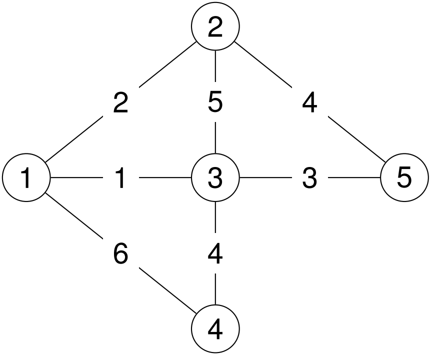
tgg22@cam.ac.uk
Computer Laboratory
University of Cambridge, UK

SBRC 2019

The Plan

- Part I : Classical Semiring-based path finding
- Part II : Drop distributivity. Show that Dijkstra's algorithm computes local optima (Sobrinho & Griffin 2010)

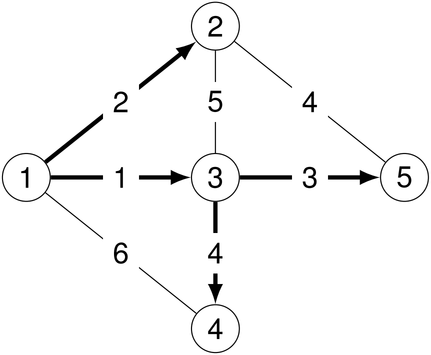
Shortest paths example, $\mathrm{sp} = (\mathbb{N}^{\infty},\ \min,\ +, \infty,\ 0)$



The adjacency matrix

$$
\mathbf{A} \quad = \quad \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array}
\begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\
\left[\begin{array}{ccccc}
\infty & 2 & 1 & 6 & \infty \\
2 & \infty & 5 & \infty & 4 \\
1 & 5 & \infty & 4 & 3 \\
6 & \infty & 4 & \infty & \infty \\
\infty & 4 & 3 & \infty & \infty
\end{array} \right] \end{array}
$$

Shortest paths solution



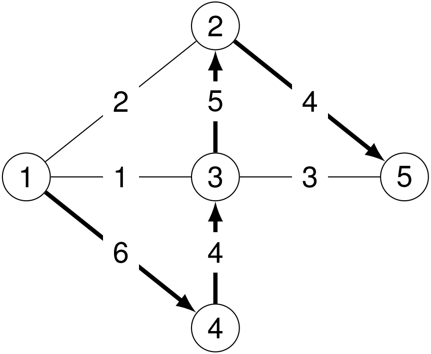
$$\mathbf{A}^* \quad = \quad \begin{array}{c|c} & \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} & \left[\begin{array}{ccccc} 0 & 2 & 1 & 5 & 4 \\ 2 & 0 & 3 & 7 & 4 \\ 1 & 3 & 0 & 4 & 3 \\ 5 & 7 & 4 & 0 & 7 \\ 4 & 4 & 3 & 7 & 0 \end{array}\right] \end{array}$$

solves this global optimality problem:

$$\mathbf{A}^*(i,\ j) = \min_{p \in \pi(i,\ j)} w(p),$$

where $\pi(i,\ j)$ is the set of all paths from i to j.

Widest paths example, $\mathrm{bw} = (\mathbb{N}^{\infty},\ \max,\ \min,\ 0,\ \infty)$



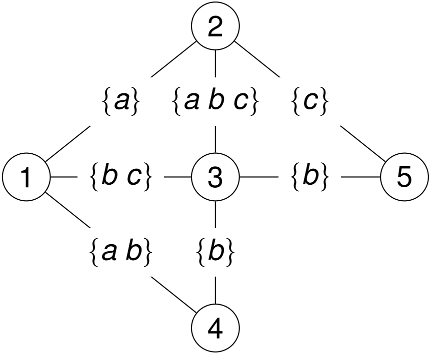
$$
\mathbf{A}^* \quad = \quad \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} \infty & 4 & 4 & 6 & 4 \\ 4 & \infty & 5 & 4 & 4 \\ 4 & 5 & \infty & 4 & 4 \\ 6 & 4 & 4 & \infty & 4 \\ 4 & 4 & 4 & 4 & \infty \end{bmatrix} \end{array}
$$

solves this global optimality problem:

$$\mathbf{A}^*(i,\ j) = \max_{p \in \pi(i,\ j)} w(p),$$

where $w(p)$ is now the minimal edge weight in p.

Unfamiliar example, $(2^{\{a,\ b,\ c\}},\ \cup,\ \cap, \{\}, \{a,\ b,\ c\})$



We want $\mathbf{A}^*$ to solve this global optimality problem:

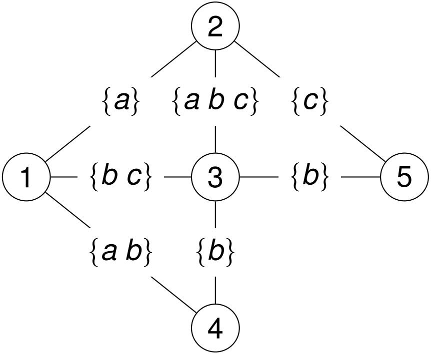
$$\mathbf{A}^*(i,\ j) = \bigcup_{p \in \pi(i,\ j)} w(p),$$

where $w(p)$ is now the intersection of all edge weights in p.

For $x \in \{a,\ b,\ c\}$, interpret $x \in \mathbf{A}^*(i,\ j)$ to mean that there is at least one path from i to j with x in every arc weight along the path.

$$\mathbf{A}^*(4,\ 1) = \{a,\ b\} \qquad \mathbf{A}^*(4,\ 5) = \{b\}$$

Another unfamiliar example, $(2^{\{a,\ b,\ c\}},\ \cap,\ \cup)$



We want matrix **R** to solve this global optimality problem:

$$\mathbf{A}^*(i,\ j) = \bigcap_{p \in \pi(i,\ j)} w(p),$$

where $w(p)$ is now the union of all edge weights in p.

For $x \in \{a,\ b,\ c\}$, interpret $x \in \mathbf{A}^*(i,\ j)$ to mean that every path from i to j has at least one arc with weight containing x.

$$\mathbf{A}^*(4,\ 1) = \{b\} \quad \mathbf{A}^*(4,\ 5) = \{b\} \quad \mathbf{A}^*(5,\ 1) = \{\}$$

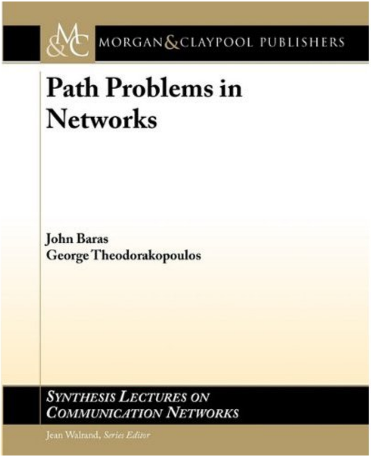
Semirings (generalise $(\mathbb{R}, +, \times, 0, 1)$)

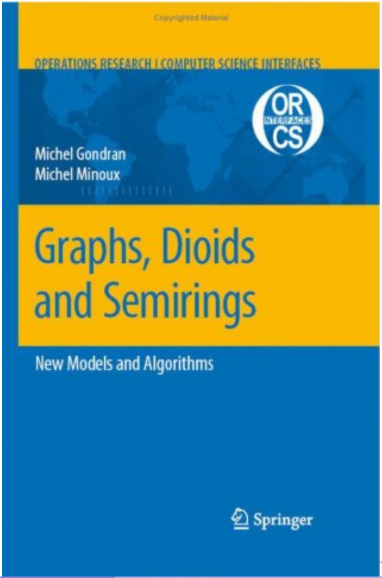
name	S	$\oplus$,	$\otimes$	$\overline{0}$	$\overline{1}$	possible routing use
sp	$\mathbb{N}^{\infty}$	min	$+$	∞	0	minimum-weight routing
bw	$\mathbb{N}^{\infty}$	max	min	0	∞	greatest-capacity routing
rel	$[0,\ 1]$	max	$\times$	0	1	most-reliable routing
use	$\{0,\ 1\}$	max	min	0	1	usable-path routing
	2^W	$\cup$	$\cap$	$\{\}$	W	shared link attributes?
	2^W	$\cap$	$\cup$	W	$\{\}$	shared path attributes?

A wee bit of notation!

Symbol	Interpretation
$\mathbb{N}$	Natural numbers (starting with zero)
$\mathbb{N}^{\infty}$	Natural numbers, plus infinity
$\overline{0}$	Identity for $\oplus$
$\overline{1}$	Identity for $\otimes$

Recommended Reading





Semigroups

Semigroup

A semigroup $(S, \ \bullet)$ is a non-empty set S with a binary operation such that

$$\mathbb{AS} \quad \text{associative} \quad \equiv \quad \forall a, b, c \in S, \ a \bullet (b \bullet c) = (a \bullet b) \bullet c$$

Some Important Semigroup Properties

$$\begin{array}{ccll}
\mathbb{ID} & \text{identity} & \equiv & \exists \alpha \in S, \ \forall a \in S, \ a = \alpha \bullet a = a \bullet \alpha \\
\mathbb{AN} & \text{annihilator} & \equiv & \exists \omega \in S, \ \forall a \in S, \ \omega = \omega \bullet a = a \bullet \omega \\
\mathbb{CM} & \text{commutative} & \equiv & \forall a, b \in S, \ a \bullet b = b \bullet a \\
\mathbb{SL} & \text{selective} & \equiv & \forall a, b \in S, \ a \bullet b \in \{a, \ b\} \\
\mathbb{IP} & \text{idempotent} & \equiv & \forall a \in S, \ a \bullet a = a
\end{array}$$

A semigroup with an identity is called a monoid.

A few concrete semigroups

S	$\bullet$	description	α	ω	$\mathbb{CM}$	$\mathbb{SL}$	$\mathbb{IP}$
S	left	x left $y = x$				$\star$	$\star$
S	right	x right $y = y$				$\star$	$\star$
S^*	$\cdot$	concatenation	ϵ				
S^+	$\cdot$	concatenation					
$\{t,\ f\}$	$\wedge$	conjunction	t	f	$\star$	$\star$	$\star$
$\{t,\ f\}$	$\vee$	disjunction	f	t	$\star$	$\star$	$\star$
$\mathbb{N}$	min	minimum		0	$\star$	$\star$	$\star$
$\mathbb{N}$	max	maximum	0		$\star$	$\star$	$\star$
2^W	$\cup$	union	$\{\}$	W	$\star$		$\star$
2^W	$\cap$	intersection	W	$\{\}$	$\star$		$\star$
$\mathrm{fin}(2^U)$	$\cup$	union	$\{\}$		$\star$		$\star$
$\mathrm{fin}(2^U)$	$\cap$	intersection		$\{\}$	$\star$		$\star$
$\mathbb{N}$	$+$	addition	0		$\star$		
$\mathbb{N}$	$\times$	multiplication	1	0	$\star$		

W a finite set, U an infinite set. For set Y, $\mathrm{fin}(Y) \equiv \{X \in Y \mid X \text{ is finite}\}$

Order Relations

We are interested in order relations $\leqslant \subseteq S \times S$

Definition (Important Order Properties)

$$
\begin{array}{lrcl}
\mathbb{RX} & \text{reflexive} & \equiv & a \leqslant a \\
\mathbb{TR} & \text{transitive} & \equiv & a \leqslant b \wedge b \leqslant c \rightarrow a \leqslant c \\
\mathbb{AY} & \text{antisymmetric} & \equiv & a \leqslant b \wedge b \leqslant a \rightarrow a = b \\
\mathbb{TO} & \text{total} & \equiv & a \leqslant b \vee b \leqslant a
\end{array}
$$

	pre-order	partial order	preference order	total order
$\mathbb{RX}$	⋆	⋆	⋆	⋆
$\mathbb{TR}$	⋆	⋆	⋆	⋆
$\mathbb{AY}$		⋆		⋆
$\mathbb{TO}$			⋆	⋆

Natural Orders

Definition (Natural orders)

Let $(S, \bullet)$ be a semigroup.

$$
\begin{array}{rcl}
a \leqslant^{L}_{\bullet} b & \equiv & a = a \bullet b \\
a \leqslant^{R}_{\bullet} b & \equiv & b = a \bullet b
\end{array}
$$

Special elements and natural orders

Lemma (Natural Bounds)

- *If α exists, then for all a, $a \leqslant_\bullet^L \alpha$ and $\alpha \leqslant_\bullet^R a$*
- *If ω exists, then for all a, $\omega \leqslant_\bullet^L a$ and $a \leqslant_\bullet^R \omega$*
- *If α and ω exist, then S is bounded.*

$$
\begin{array}{ccccc}
\omega & \leqslant_\bullet^L & a & \leqslant_\bullet^L & \alpha \\
\alpha & \leqslant_\bullet^R & a & \leqslant_\bullet^R & \omega
\end{array}
$$

Remark (Thanks to Iljitsch van Beijnum)

Note that this means for $(\min, +)$ we have

$$
\begin{array}{ccccc}
0 & \leqslant_{\min}^L & a & \leqslant_{\min}^L & \infty \\
\infty & \leqslant_{\min}^R & a & \leqslant_{\min}^R & 0
\end{array}
$$

and still say that this is bounded, even though one might argue with the terminology!

Examples of special elements

S	$\bullet$	α	ω	$\leqslant^{\mathrm{L}}_{\bullet}$	$\leqslant^{\mathrm{R}}_{\bullet}$
$\mathbb{N}^{\infty}$	min	∞	0	$\leqslant$	$\geqslant$
$\mathbb{N}^{-\infty}$	max	0	$-\infty$	$\geqslant$	$\leqslant$
$\mathcal{P}(W)$	$\cup$	$\{\}$	W	$\subseteq$	$\supseteq$
$\mathcal{P}(W)$	$\cap$	W	$\{\}$	$\supseteq$	$\subseteq$

Property Management

Lemma

Let $D \in \{R,\ L\}$.

1. $\mathbb{IP}(S,\ \bullet) \iff \mathbb{RX}(S,\ \leqslant_{\bullet}^{D})$
2. $\mathbb{CM}(S,\ \bullet) \implies \mathbb{AY}(S,\ \leqslant_{\bullet}^{D})$
3. $\mathbb{AS}(S,\ \bullet) \implies \mathbb{TR}(S,\ \leqslant_{\bullet}^{D})$
4. $\mathbb{CM}(S,\ \bullet) \implies (\mathbb{SL}(S,\ \bullet) \iff \mathbb{TO}(S,\ \leqslant_{\bullet}^{D}))$

Proof.

1. $a \leqslant_{\bullet}^{D} a \iff a = a \bullet a,$
2. $a \leqslant_{\bullet}^{L} b \wedge b \leqslant_{\bullet}^{L} a \iff a = a \bullet b \wedge b = b \bullet a \implies a = b$
3. $a \leqslant_{\bullet}^{L} b \wedge b \leqslant_{\bullet}^{L} c \iff a = a \bullet b \wedge b = b \bullet c \implies a = a \bullet (b \bullet c) = (a \bullet b) \bullet c = a \bullet c \implies a \leqslant_{\bullet}^{L} c$
4. $a = a \bullet b \vee b = a \bullet b \iff a \leqslant_{\bullet}^{L} b \vee b \leqslant_{\bullet}^{L} a$

$\square$

Bi-semigroups and Pre-Semirings

$(S, \oplus, \otimes)$ is a bi-semigroup when

- $(S, \oplus)$ is a semigroup
- $(S, \otimes)$ is a semigroup

$(S, \oplus, \otimes)$ is a pre-semiring when

- $(S, \oplus, \otimes)$ is a bi-semigroup
- $\oplus$ is commutative

and left- and right-distributivity hold,

$$\begin{array}{lcrcl} \mathbb{LD} & : & a \otimes (b \oplus c) & = & (a \otimes b) \oplus (a \otimes c) \\ \mathbb{RD} & : & (a \oplus b) \otimes c & = & (a \otimes c) \oplus (b \otimes c) \end{array}$$

Semirings

$(S, \oplus, \otimes, \overline{0}, \overline{1})$ is a semiring when

- $(S, \oplus, \otimes)$ is a pre-semiring
- $(S, \oplus, \overline{0})$ is a (commutative) monoid
- $(S, \otimes, \overline{1})$ is a monoid
- $\overline{0}$ is an annihilator for $\otimes$

Examples

Pre-semirings

name	S	$\oplus$,	$\otimes$	$\overline{0}$	$\overline{1}$
min_plus	$\mathbb{N}$	min	$+$		0
max_min	$\mathbb{N}$	max	min	0	

Semirings

name	S	$\oplus$,	$\otimes$	$\overline{0}$	$\overline{1}$
sp	$\mathbb{N}^{\infty}$	min	$+$	∞	0
bw	$\mathbb{N}^{\infty}$	max	min	0	∞

Note the sloppiness — the symbols $+$, max, and min in the two tables represent different functions....

Matrix Semirings

- $(S, \oplus, \otimes, \overline{0}, \overline{1})$ a semiring
- Define the semiring of $n \times n$-matrices over S : $(\mathbb{M}_n(S), \oplus, \otimes, \mathbf{J}, \mathbf{I})$

$\oplus$ and $\otimes$

$$
\begin{aligned}
(\mathbf{A} \oplus \mathbf{B})(i, j) &= \mathbf{A}(i, j) \oplus \mathbf{B}(i, j) \\
(\mathbf{A} \otimes \mathbf{B})(i, j) &= \bigoplus_{1 \leqslant q \leqslant n} \mathbf{A}(i, q) \otimes \mathbf{B}(q, j)
\end{aligned}
$$

J and I

$$
\begin{aligned}
\mathbf{J}(i, j) &= \overline{0} \\
\mathbf{I}(i, j) &= \begin{cases} \overline{1} & (\text{if } i = j) \\ \overline{0} & (\text{otherwise}) \end{cases}
\end{aligned}
$$

Associativity

$$\mathbf{A} \otimes (\mathbf{B} \otimes \mathbf{C}) = (\mathbf{A} \otimes \mathbf{B}) \otimes \mathbf{C}$$

$$\begin{array}{lll}
 & (\mathbf{A} \otimes (\mathbf{B} \otimes \mathbf{C}))(i,\ j) & \\
= & \bigoplus_{1 \leqslant u \leqslant n} \mathbf{A}(i,\ u) \otimes (\mathbf{B} \otimes \mathbf{C})(u,\ j) & (\text{def} \rightarrow) \\
= & \bigoplus_{1 \leqslant u \leqslant n} \mathbf{A}(i,\ u) \otimes (\bigoplus_{1 \leqslant v \leqslant n} \mathbf{B}(u,\ v) \otimes \mathbf{C}(v,\ j)) & (\text{def} \rightarrow) \\
= & \bigoplus_{1 \leqslant u \leqslant n} \bigoplus_{1 \leqslant v \leqslant n} \mathbf{A}(i,\ u) \otimes (\mathbf{B}(u,\ v) \otimes \mathbf{C}(v,\ j)) & (\mathbb{LD}) \\
= & \bigoplus_{1 \leqslant v \leqslant n} \bigoplus_{1 \leqslant u \leqslant n} (\mathbf{A}(i,\ u) \otimes \mathbf{B}(u,\ v)) \otimes \mathbf{C}(v,\ j) & (\mathbb{AS}, \mathbb{CM}) \\
= & \bigoplus_{1 \leqslant v \leqslant n} (\bigoplus_{1 \leqslant u \leqslant n} \mathbf{A}(i,\ u) \otimes \mathbf{B}(u,\ v)) \otimes \mathbf{C}(v,\ j) & (\mathbb{RD}) \\
= & \bigoplus_{1 \leqslant v \leqslant n} (\mathbf{A} \otimes \mathbf{B})(i,\ v) \otimes \mathbf{C}(v,\ j) & (\text{def} \leftarrow) \\
= & ((\mathbf{A} \otimes \mathbf{B}) \otimes \mathbf{C})(i,\ j) & (\text{def} \leftarrow)
\end{array}$$

Left Distributivity

$$\mathbf{A} \otimes (\mathbf{B} \oplus \mathbf{C}) = (\mathbf{A} \otimes \mathbf{B}) \oplus (\mathbf{A} \otimes \mathbf{C})$$

$$\begin{array}{lll}
 & (\mathbf{A} \otimes (\mathbf{B} \oplus \mathbf{C}))(i,\ j) & \\
= & \bigoplus_{1 \leqslant q \leqslant n} \mathbf{A}(i,\ q) \otimes (\mathbf{B} \oplus \mathbf{C})(q,\ j) & (\mathrm{def} \rightarrow) \\
= & \bigoplus_{1 \leqslant q \leqslant n} \mathbf{A}(i,\ q) \otimes (\mathbf{B}(q,\ j) \oplus \mathbf{C}(q,\ j)) & (\mathrm{def} \rightarrow) \\
= & \bigoplus_{1 \leqslant q \leqslant n} (\mathbf{A}(i,\ q) \otimes \mathbf{B}(q,\ j)) \oplus (\mathbf{A}(i,\ q) \otimes \mathbf{C}(q,\ j)) & (\mathbb{LD}) \\
= & (\bigoplus_{1 \leqslant q \leqslant n} \mathbf{A}(i,\ q) \otimes \mathbf{B}(q,\ j)) \oplus (\bigoplus_{1 \leqslant q \leqslant n} \mathbf{A}(i,\ q) \otimes \mathbf{C}(q,\ j)) & (\mathbb{AS}, \mathbb{CM}) \\
= & ((\mathbf{A} \otimes \mathbf{B}) \oplus (\mathbf{A} \otimes \mathbf{C}))(i,\ j) & (\mathrm{def} \leftarrow)
\end{array}$$

Matrix encoding path problems

- $(S, \oplus, \otimes, \overline{0}, \overline{1})$ a semiring
- $G = (V, E)$ a directed graph
- $w \in E \rightarrow S$ a weight function

Path weight

The <u>weight</u> of a path $p = i_1, i_2, i_3, \cdots, i_k$ is

$$w(p) = w(i_1, i_2) \otimes w(i_2, i_3) \otimes \cdots \otimes w(i_{k-1}, i_k).$$

The empty path is given the weight $\overline{1}$.

Adjacency matrix **A**

$$\mathbf{A}(i, j) = \begin{cases} w(i, j) & \text{if } (i, j) \in E, \\ \overline{0} & \text{otherwise} \end{cases}$$

The general problem of finding globally optimal path weights

Given an adjacency matrix $\mathbf{A}$, find $\mathbf{A}^*$ such that for all $i,\ j \in V$

$$\mathbf{A}^*(i,\ j) = \bigoplus_{p \in \pi(i,\ j)} w(p)$$

where $\pi(i,\ j)$ represents the set of all paths from i to j.

How can we solve this problem?

Stability

- $(S, \oplus, \otimes, \overline{0}, \overline{1})$ a semiring

$a \in S$, define powers a^k

$$\begin{aligned} a^0 &= \overline{1} \\ a^{k+1} &= a \otimes a^k \end{aligned}$$

Closure, a^*

$$\begin{aligned} a^{(k)} &= a^0 \oplus a^1 \oplus a^2 \oplus \cdots \oplus a^k \\ a^* &= a^0 \oplus a^1 \oplus a^2 \oplus \cdots \oplus a^k \oplus \cdots \end{aligned}$$

Definition (q stability)

If there exists a q such that $a^{(q)} = a^{(q+1)}$, then a is q-stable. By induction: $\forall t, 0 \leqslant t, a^{(q+t)} = a^{(q)}$. Therefore, $a^* = a^{(q)}$.

Matrix methods

Matrix powers, $\mathbf{A}^k$

$$\begin{aligned} \mathbf{A}^0 &= \mathbf{I} \\ \mathbf{A}^{k+1} &= \mathbf{A} \otimes \mathbf{A}^k \end{aligned}$$

Closure, $\mathbf{A}^*$

$$\begin{aligned} \mathbf{A}^{(k)} &= \mathbf{I} \oplus \mathbf{A}^1 \oplus \mathbf{A}^2 \oplus \cdots \oplus \mathbf{A}^k \\ \mathbf{A}^* &= \mathbf{I} \oplus \mathbf{A}^1 \oplus \mathbf{A}^2 \oplus \cdots \oplus \mathbf{A}^k \oplus \cdots \end{aligned}$$

Note: $\mathbf{A}^*$ might not exist. Why?

Matrix methods can compute optimal path weights

- Let $\pi(i, j)$ be the set of paths from i to j.
- Let $\pi^k(i, j)$ be the set of paths from i to j with exactly k arcs.
- Let $\pi^{(k)}(i, j)$ be the set of paths from i to j with at most k arcs.

Theorem

$$
\begin{array}{lrcl}
(1) & \mathbf{A}^k(i,\ j) & = & \bigoplus_{p \in \pi^k(i,\ j)} w(p) \\
(2) & \mathbf{A}^{(k)}(i,\ j) & = & \bigoplus_{p \in \pi^{(k)}(i,\ j)} w(p) \\
(3) & \mathbf{A}^*(i,\ j) & = & \bigoplus_{p \in \pi(i,\ j)} w(p)
\end{array}
$$

Warning again: for some semirings the expression $\mathbf{A}^*(i,\ j)$ might not be well-defeind. Why?

Proof of (1)

By induction on k. Base Case: $k = 0$.

$$\pi^0(i,\ i) = \{\epsilon\},$$

so $\mathbf{A}^0(i\ , i) = \mathbf{I}(i,\ i) = \overline{1} = w(\epsilon)$.

And $i \neq j$ implies $\pi^0(i, j) = \{\}$. By convention

$$\bigoplus_{p \in \{\}} w(p) = \overline{0} = \mathbf{I}(i,\ j).$$

Proof of (1)

Induction step.

$$
\begin{aligned}
\mathbf{A}^{k+1}(i,j) &= (\mathbf{A} \otimes \mathbf{A}^k)(i,\ j) \\
&= \bigoplus_{1 \leqslant q \leqslant n} \mathbf{A}(i,\ q) \otimes \mathbf{A}^k(q,\ j) \\
&= \bigoplus_{1 \leqslant q \leqslant n} \mathbf{A}(i,\ q) \otimes (\bigoplus_{p \in \pi^k(q,\ j)} w(p)) \\
&= \bigoplus_{1 \leqslant q \leqslant n} \bigoplus_{p \in \pi^k(q,\ j)} \mathbf{A}(i,\ q) \otimes w(p) \\
&= \bigoplus_{(i,\ q) \in E} \bigoplus_{p \in \pi^k(q,j)} w(i,\ q) \otimes w(p) \\
&= \bigoplus_{p \in \pi^{k+1}(i,\ j)} w(p)
\end{aligned}
$$

Fun Facts

Fact 3

If $\overline{1}$ is an annihiltor for $\oplus$, then every $a \in S$ is 0-stable!

Fact 4

If S is 0-stable, then $\mathbb{M}_n(S)$ is $(n-1)$-stable. That is,

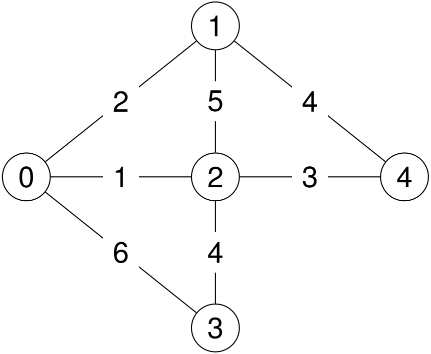
$$\mathbf{A}^* = \mathbf{A}^{(n-1)} = \mathbf{I} \oplus \mathbf{A}^1 \oplus \mathbf{A}^2 \oplus \cdots \oplus \mathbf{A}^{n-1}$$

Why? Because we can ignore paths with loops.

$$(a \otimes c \otimes b) \oplus (a \otimes b) = a \otimes (\overline{1} \oplus c) \otimes b = a \otimes \overline{1} \otimes b = a \otimes b$$

Think of c as the weight of a loop in a path with weight $a \otimes b$.

Shortest paths example, $(\mathbb{N}^{\infty}, \min, +)$



The adjacency matrix

$$\mathbf{A} = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \left[\begin{array}{ccccc} \infty & 2 & 1 & 6 & \infty \\ 2 & \infty & 5 & \infty & 4 \\ 1 & 5 & \infty & 4 & 3 \\ 6 & \infty & 4 & \infty & \infty \\ \infty & 4 & 3 & \infty & \infty \end{array} \right] \end{array}$$

Note that the longest shortest path is $(1, 0, 2, 3)$ of length 3 and weight 7.

$(\min, +)$ example

Our theorem tells us that $\mathbf{A}^* = \mathbf{A}^{(n-1)} = \mathbf{A}^{(4)}$

$$\mathbf{A}^* = \mathbf{A}^{(4)} = \mathbf{I} \;\min\; \mathbf{A} \;\min\; \mathbf{A}^2 \;\min\; \mathbf{A}^3 \;\min\; \mathbf{A}^4 = \begin{array}{c c} & \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} & \left[\begin{array}{ccccc} 0 & 2 & 1 & 5 & 4 \\ 2 & 0 & 3 & 7 & 4 \\ 1 & 3 & 0 & 4 & 3 \\ 5 & 7 & 4 & 0 & 7 \\ 4 & 4 & 3 & 7 & 0 \end{array}\right] \end{array}$$

$(\min, +)$ example

$$\mathbf{A} = \begin{array}{c|ccccc} & 0 & 1 & 2 & 3 & 4 \\ \hline 0 & \infty & \underline{2} & \underline{1} & 6 & \infty \\ 1 & \underline{2} & \infty & 5 & \infty & \underline{4} \\ 2 & \underline{1} & 5 & \infty & \underline{4} & \underline{3} \\ 3 & 6 & \infty & \underline{4} & \infty & \infty \\ 4 & \infty & \underline{4} & \underline{3} & \infty & \infty \end{array}$$

$$\mathbf{A}^3 = \begin{array}{c|ccccc} & 0 & 1 & 2 & 3 & 4 \\ \hline 0 & 8 & 4 & 3 & 8 & 10 \\ 1 & 4 & 8 & 7 & \underline{7} & 6 \\ 2 & 3 & 7 & 8 & 6 & 5 \\ 3 & 8 & \underline{7} & 6 & 11 & 10 \\ 4 & 10 & 6 & 5 & 10 & 12 \end{array}$$

$$\mathbf{A}^2 = \begin{array}{c|ccccc} & 0 & 1 & 2 & 3 & 4 \\ \hline 0 & 2 & 6 & 7 & \underline{5} & \underline{4} \\ 1 & 6 & 4 & \underline{3} & 8 & 8 \\ 2 & 7 & \underline{3} & 2 & 7 & 9 \\ 3 & \underline{5} & 8 & 7 & 8 & \underline{7} \\ 4 & \underline{4} & 8 & 9 & \underline{7} & 6 \end{array}$$

$$\mathbf{A}^4 = \begin{array}{c|ccccc} & 0 & 1 & 2 & 3 & 4 \\ \hline 0 & 4 & 8 & 9 & 7 & 6 \\ 1 & 8 & 6 & 5 & 10 & 10 \\ 2 & 9 & 5 & 4 & 9 & 11 \\ 3 & 7 & 10 & 9 & 10 & 9 \\ 4 & 6 & 10 & 11 & 9 & 8 \end{array}$$

First appearance of final value is in red and <u>underlined</u>. Remember: we are looking at all paths of a given length, even those with cycles!

$\mathbf{A}$ vs $\mathbf{A} \oplus \mathbf{I}$

Lemma

If $\oplus$ is idempotent, then

$$(\mathbf{A} \oplus \mathbf{I})^k = \mathbf{A}^{(k)}.$$

Proof. Base case: When $k = 0$ both expressions are $\mathbf{I}$.
Assume $(\mathbf{A} \oplus \mathbf{I})^k = \mathbf{A}^{(k)}$. Then

$$\begin{aligned}
(\mathbf{A} \oplus \mathbf{I})^{k+1} &= (\mathbf{A} \oplus \mathbf{I})(\mathbf{A} \oplus \mathbf{I})^k \\
&= (\mathbf{A} \oplus \mathbf{I})\mathbf{A}^{(k)} \\
&= \mathbf{A}\mathbf{A}^{(k)} \oplus \mathbf{A}^{(k)} \\
&= \mathbf{A}(\mathbf{I} \oplus \mathbf{A} \oplus \cdots \oplus \mathbf{A}^k) \oplus \mathbf{A}^{(k)} \\
&= \mathbf{A} \oplus \mathbf{A}^2 \oplus \cdots \oplus \mathbf{A}^{k+1} \oplus \mathbf{A}^{(k)} \\
&= \mathbf{A}^{k+1} \oplus \mathbf{A}^{(k)} \\
&= \mathbf{A}^{(k+1)}
\end{aligned}$$

back to $(\min, +)$ example

$$(\mathbf{A} \oplus \mathbf{I})^1 = \begin{array}{c c} & \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{bmatrix} 0 & 2 & 1 & 6 & \infty \\ 2 & 0 & 5 & \infty & 4 \\ 1 & 5 & 0 & 4 & 3 \\ 6 & \infty & 4 & 0 & \infty \\ \infty & 4 & 3 & \infty & 0 \end{bmatrix} \end{array}$$

$$(\mathbf{A} \oplus \mathbf{I})^3 = \begin{array}{c c} & \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{bmatrix} 0 & 2 & 1 & 5 & 4 \\ 2 & 0 & 3 & 7 & 4 \\ 1 & 3 & 0 & 4 & 3 \\ 5 & 7 & 4 & 0 & 7 \\ 4 & 4 & 3 & 7 & 0 \end{bmatrix} \end{array}$$

$$(\mathbf{A} \oplus \mathbf{I})^2 = \begin{array}{c c} & \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{bmatrix} 0 & 2 & 1 & 5 & 4 \\ 2 & 0 & 3 & 8 & 4 \\ 1 & 3 & 0 & 4 & 3 \\ 5 & 8 & 4 & 0 & 7 \\ 4 & 4 & 3 & 7 & 0 \end{bmatrix} \end{array}$$

Solving (some) equations

Theorem 6.1

If $\mathbf{A}$ is q-stable, then $\mathbf{A}^*$ solves the equations

$$\mathbf{L} = \mathbf{A}\mathbf{L} \oplus \mathbf{I}$$

and

$$\mathbf{R} = \mathbf{R}\mathbf{A} \oplus \mathbf{I}.$$

For example, to show $\mathbf{L} = \mathbf{A}^*$ solves the first equation:

$$\begin{array}{rcl}
\mathbf{A}^* & = & \mathbf{A}^{(q)} \\
 & = & \mathbf{A}^{(q+1)} \\
 & = & \mathbf{A}^{q+1} \oplus \mathbf{A}^{q} \oplus \ldots \oplus \mathbf{A}^{2} \oplus \mathbf{A} \oplus \mathbf{I} \\
 & = & \mathbf{A}(\mathbf{A}^{q} \oplus \mathbf{A}^{q-1} \oplus \ldots \oplus \mathbf{A} \oplus \mathbf{I}) \oplus \mathbf{I} \\
 & = & \mathbf{A}\mathbf{A}^{(q)} \oplus \mathbf{I} \\
 & = & \mathbf{A}\mathbf{A}^{*} \oplus \mathbf{I}
\end{array}$$

Note that if we replace the assumption "**A** is q-stable" with "$\mathbf{A}^*$ exists," then we require that $\otimes$ distributes over infinite sums.

A more general result

Theorem Left-Right

If $\mathbf{A}$ is q-stable, then $\mathbf{L} = \mathbf{A}^*\mathbf{B}$ solves the equation

$$\mathbf{L} = \mathbf{A}\mathbf{L} \oplus \mathbf{B}$$

and $\mathbf{R} = \mathbf{B}\mathbf{A}^*$ solves

$$\mathbf{R} = \mathbf{R}\mathbf{A} \oplus \mathbf{B}.$$

For the first equation:

$$\begin{aligned}
\mathbf{A}^*\mathbf{B} &= \mathbf{A}^{(q)}\mathbf{B} \\
&= \mathbf{A}^{(q+1)}\mathbf{B} \\
&= (\mathbf{A}^{q+1} \oplus \mathbf{A}^{q} \oplus \ldots \oplus \mathbf{A}^{2} \oplus \mathbf{A} \oplus \mathbf{I})\mathbf{B} \\
&= (\mathbf{A}^{q+1} \oplus \mathbf{A}^{q} \oplus \ldots \oplus \mathbf{A}^{2} \oplus \mathbf{A})\mathbf{B} \oplus \mathbf{B} \\
&= \mathbf{A}(\mathbf{A}^{q} \oplus \mathbf{A}^{q-1} \oplus \ldots \oplus \mathbf{A} \oplus \mathbf{I})\mathbf{B} \oplus \mathbf{B} \\
&= \mathbf{A}(\mathbf{A}^{(q)}\mathbf{B}) \oplus \mathbf{B} \\
&= \mathbf{A}(\mathbf{A}^*\mathbf{B}) \oplus \mathbf{B}
\end{aligned}$$

The “best” solution

Suppose $\mathbf{Y}$ is a matrix such that

$$\mathbf{Y} = \mathbf{AY} \oplus \mathbf{I}$$

$$\begin{array}{rcl} \mathbf{Y} & = & \mathbf{AY} \oplus \mathbf{I} \\ & = & \mathbf{A}^1\mathbf{Y} \oplus \mathbf{A}^{(0)} \\ & = & \mathbf{A}((\mathbf{AY} \oplus \mathbf{I})) \oplus \mathbf{I} \\ & = & \mathbf{A}^2\mathbf{Y} \oplus \mathbf{A} \oplus \mathbf{I} \\ & = & \mathbf{A}^2\mathbf{Y} \oplus \mathbf{A}^{(1)} \\ \vdots & & \vdots \quad \vdots \\ & = & \mathbf{A}^{k+1}\mathbf{Y} \oplus \mathbf{A}^{(k)} \end{array}$$

If $\mathbf{A}$ is q-stable and $q < k$, then

$$\mathbf{Y} = \mathbf{A}^k\mathbf{Y} \oplus \mathbf{A}^*$$

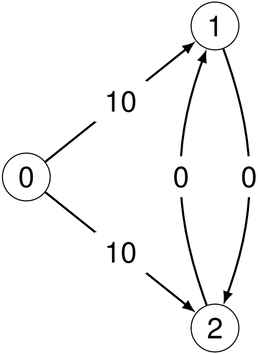
$$\mathbf{Y} \trianglelefteq^L_\oplus \mathbf{A}^*$$

and if $\oplus$ is idempotent, then

$$\mathbf{Y} \leqslant^L_\oplus \mathbf{A}^*$$

So $\mathbf{A}^*$ is the largest solution. What does this mean in terms of the sp semiring?

Example with zero weighted cycles using sp semiring



$$\mathbf{A} = \begin{array}{c|ccc} & 0 & 1 & 2 \\ \hline 0 & \infty & 10 & 10 \\ 1 & \infty & \infty & 0 \\ 2 & \infty & 0 & \infty \end{array}$$

$\mathbf{A}^*$ $(= \mathbf{A} \oplus \mathbf{I}$ in this case) solves

$$\mathbf{X} = \mathbf{XA} \oplus \mathbf{I}.$$

But so does this (dishonest) matrix!

$$\mathbf{F} = \begin{array}{c|ccc} & 0 & 1 & 2 \\ \hline 0 & 0 & 9 & 9 \\ 1 & \infty & 0 & 0 \\ 2 & \infty & 0 & 0 \end{array}$$

For example :

$$\begin{aligned} & (\mathbf{FA} \oplus \mathbf{I})(0, 1) \\ = & \min_{q \in \{0,1,2\}} \mathbf{F}(0, q) + \mathbf{A}(q, 1) \\ = & \min(0 + 10, 9 + \infty, 9 + 0) \\ = & 9 \\ = & \mathbf{F}(0, 1) \end{aligned}$$

An interesting semiring

Let $G = (V, E)$ be a directed graph.

Cut Sets

- A cut set $C \subseteq E$ for nodes i and j is a set of arcs such there is no path from i to j in the graph $(V, E - C)$.
- C is minimal if no proper subset of C is an arc cut set.

Martelli's Semiring

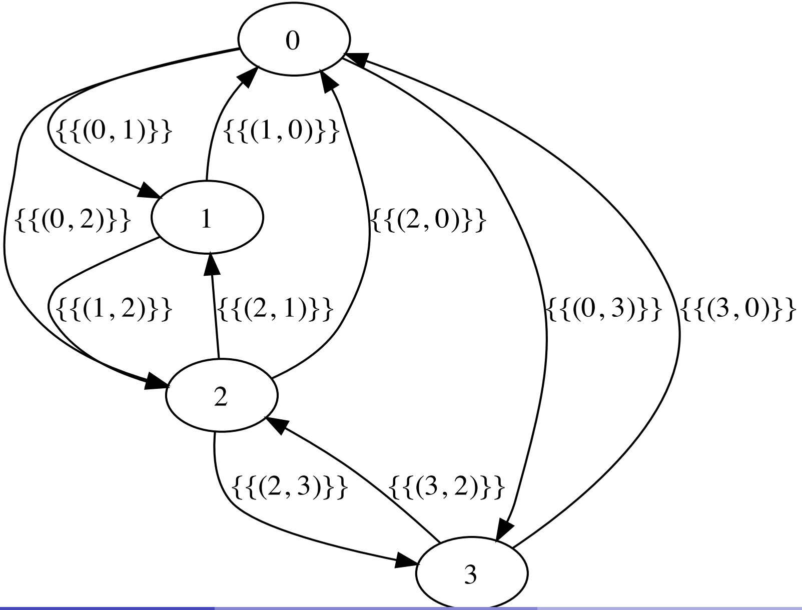
Let $G = (V,\ E)$ be a directed graph.

$$
\begin{array}{rcl}
\mathbb{M} & \equiv & (S,\ \oplus,\ \otimes,\ \overline{0},\ \overline{1}) \\
S & \equiv & \{X \in 2^{2^E} \mid \forall U, V \in X, U \subseteq V \implies U = V\} \\
X \oplus Y & \equiv & \text{remove all supersets from } \{U \cup V \mid U \in X,\ V \in Y\} \\
X \otimes Y & \equiv & \text{remove all supersets from } X \cup Y \\
\overline{0} & \equiv & \{\{\}\} \\
\overline{1} & \equiv & \{\}
\end{array}
$$

What does it do?

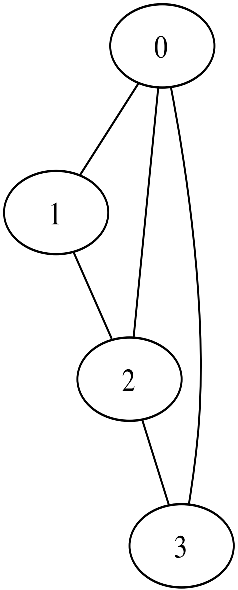
- If every arc $(i,\ j)$ is has weight $\mathbf{A}(i,\ j) = \{\{(i,\ j)\}\}$, then $\mathbf{A}^*(i,\ j)$ is the set of all minimal arc cut sets for i and j.

A



Part of $\mathbf{A}^*$

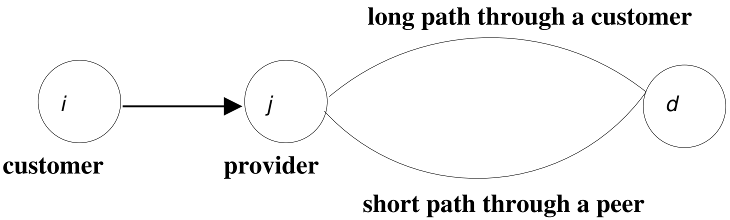
$$
\begin{aligned}
\mathbf{A}^*(0,\ 1) &= \{\{(0,1),(2,1)\},\\
&\quad \{(0,1),(0,2),(0,3)\},\\
&\quad \{(0,1),(0,2),(3,2)\}\}\\
\mathbf{A}^*(0,\ 2) &= \{\{(0,2),(1,2),(3,2)\},\\
&\quad \{(0,1),(0,2),(3,2)\},\\
&\quad \{(0,1),(0,2),(0,3)\},\\
&\quad \{(0,2),(0,3),(1,2)\}\}\\
\mathbf{A}^*(2,\ 0) &= \{\{(2,0),(2,1),(3,0)\},\\
&\quad \{(1,0),(2,0),(3,0)\},\\
&\quad \{(1,0),(2,0),(2,3)\},\\
&\quad \{(2,0),(2,1),(2,3)\}\}\\
\mathbf{A}^*(2,\ 3) &= \{\{(2,0),(2,1),(2,3)\},\\
&\quad \{(0,3),(2,3)\},\\
&\quad \{(1,0),(2,0),(2,3)\}\}
\end{aligned}
$$



Part II

Drop distributivity!

Should distributivity hold in Internet Routing?

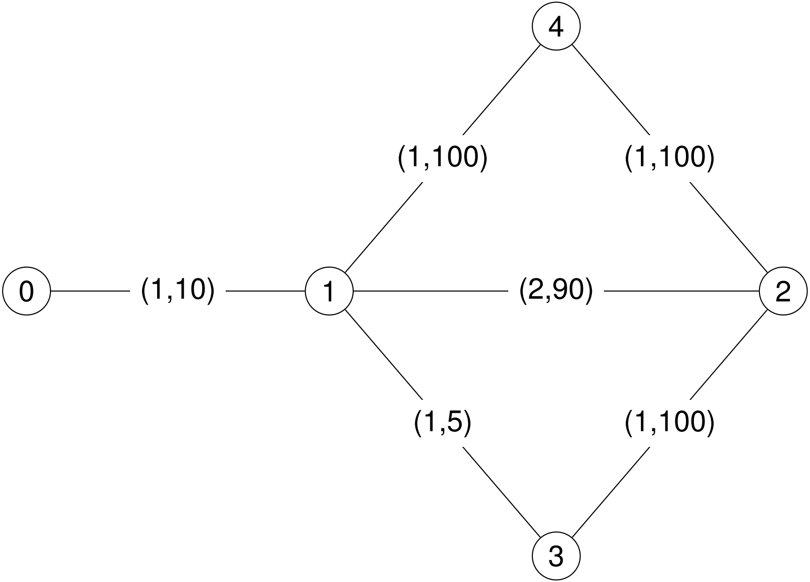


- *j* prefers long path though one of its customers (not the shorter path through a competitor)
- given two routes from a provider, *i* prefers the one with a shorter path
- More on inter-domain routing in the Internet later in the term ...

Widest shortest-paths

- Metric of the form $(d, \ b)$, where d is distance $(\min, \ +)$ and b is capacity $(\max, \ \min)$.
- Metrics are compared lexicographically, with distance considered first.
- Such things are found in the vast literature on Quality-of-Service (QoS) metrics for Internet routing.

Widest shortest-paths



Weights are globally optimal (we have a semiring)

Widest shortest-path weights computed by Dijkstra and Bellman-Ford

$$\mathbf{R} = \begin{array}{c c} & \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{bmatrix} (0, \infty) & (1, 10) & (3, 10) & (2, 5) & (2, 10) \\ (1, 10) & (0, \infty) & (2, 100) & (1, 5) & (1, 100) \\ (3, 10) & (2, 100) & (0, \infty) & (1, 100) & (1, 100) \\ (2, 5) & (1, 5) & (1, 100) & (0, \infty) & (2, 100) \\ (2, 10) & (1, 100) & (1, 100) & (2, 100) & (0, \infty) \end{bmatrix} \end{array}$$

But what about the paths themselves?

Four optimal paths of weight $(3, 10)$.

$$\begin{array}{rcl} \mathbf{P}_{\text{optimal}}(0, 2) & = & \{(0, 1, 2),\ (0, 1, 4, 2)\} \\ \mathbf{P}_{\text{optimal}}(2, 0) & = & \{(2, 1, 0),\ (2, 4, 1, 0)\} \end{array}$$

There are standard ways to extend Bellman-Ford and Dijkstra to compute paths (or the associated next hops).

Do these extended algorithms find all optimal paths?

Surprise!

Four **optimal** paths of weight $(3, 10)$

$$\begin{array}{rcl} \mathbf{P}_{\text{optimal}}(0,2) & = & \{(0,1,2),\ (0,1,4,2)\} \\ \mathbf{P}_{\text{optimal}}(2,0) & = & \{(2,1,0),\ (2,4,1,0)\} \end{array}$$

Paths computed by (extended) **Dijkstra**

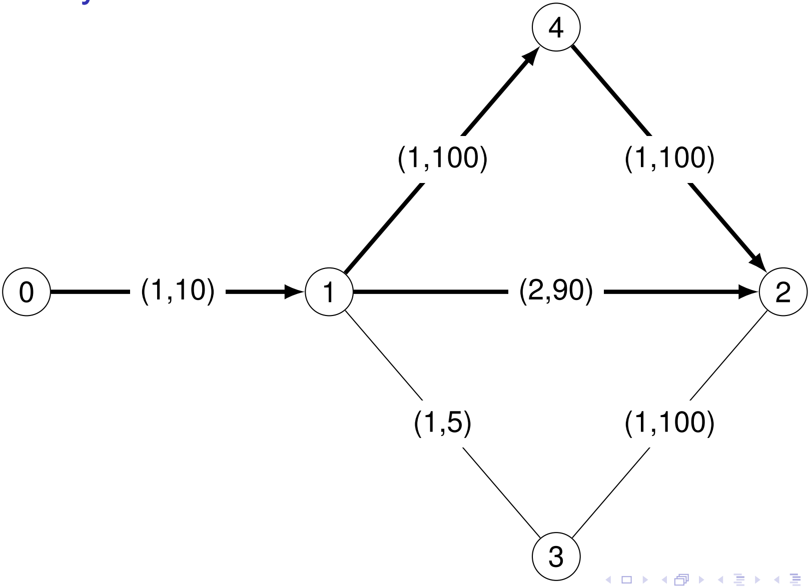
$$\begin{array}{rcl} \mathbf{P}_{\text{Dijkstra}}(0,2) & = & \{(0,1,2),\ (0,1,4,2)\} \\ \mathbf{P}_{\text{Dijkstra}}(2,0) & = & \{(2,4,1,0)\} \end{array}$$

Notice that 0's paths cannot both be implemented with next-hop forwarding since $\mathbf{P}_{\text{Dijkstra}}(1,2) = \{(1,4,2)\}$.

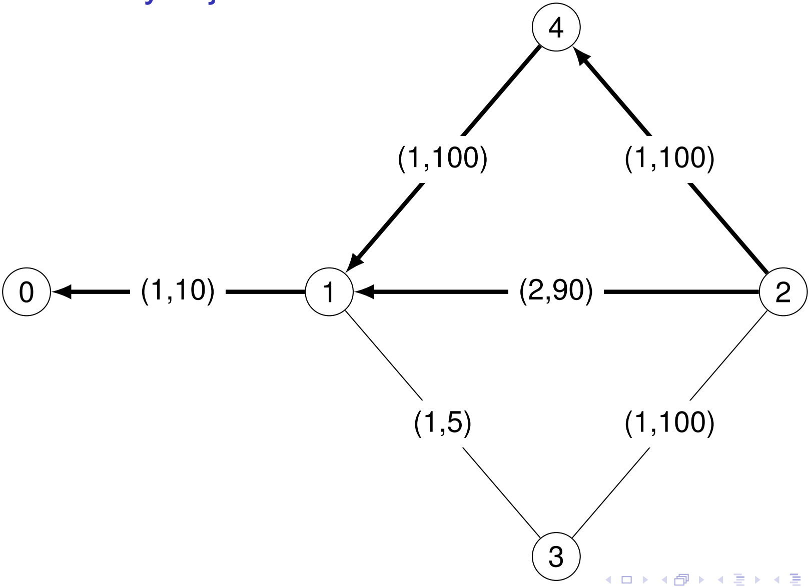
Paths computed by **distributed Bellman-Ford**

$$\begin{array}{rcl} \mathbf{P}_{\text{Bellman}}(0,2) & = & \{(0,1,4,2)\} \\ \mathbf{P}_{\text{Bellman}}(2,0) & = & \{(2,1,0),\ (2,4,1,0)\} \end{array}$$

Optimal paths from 0 to 2. Computed by Dijkstra but not by Bellman-Ford



Optimal paths from 2 to 1. Computed by Bellman-Ford but not by Dijkstra



How can we understand this (algebaically)?

The Algorithm to Algebra (A2A) method

$$\left(\begin{array}{c} \text{original metric} \\ + \\ \text{complex algorithm} \end{array} \right) \rightarrow \left(\begin{array}{c} \text{modified metric} \\ + \\ \text{matrix equations (generic algorithm)} \end{array} \right)$$

Preview

- We can add paths explicitly to the widest shortest-path semiring to obtain a new algebra.
- We will see that distributivity does not hold for this algebra.
- Why? We will see that it is because min is not cancellative! ($a \min b = a \min c$ does not imply that $b = c$)

Towards a non-classical theory of algebraic path finding

We need theory that can accept algebras that violate distributivity.

Global optimality

$$\mathbf{A}^*(i,\ j) = \bigoplus_{p \in P(i,\ j)} w(p),$$

Left local optimality (distributed Bellman-Ford)

$$\mathbf{L} = (\mathbf{A} \otimes \mathbf{L}) \oplus \mathbf{I}.$$

Right local optimality (Dijkstra's Algorithm)

$$\mathbf{R} = (\mathbf{R} \otimes \mathbf{A}) \oplus \mathbf{I}.$$

Embrace the fact that all three notions can be distinct.

Dijkstra's Algorithm

Classical Dijkstra

Given adjacency matrix **A** over a selective semiring and source vertex $i \in V$, Dijkstra's algorithm will compute $\mathbf{A}^*(i, \_)$ such that

$$\mathbf{A}^*(i, j) = \bigoplus_{p \in P(i,j)} w_{\mathbf{A}}(p).$$

Non-Classical Dijkstra

If we drop assumptions of distributivity, then given adjacency matrix **A** and source vertex $i \in V$, Dijkstra's algorithm will compute $\mathbf{R}(i, \_)$ such that

$$\forall j \in V : \mathbf{R}(i, j) = \mathbf{I}(i,j) \oplus \bigoplus_{q \in V} \mathbf{R}(i, q) \otimes \mathbf{A}(q, j).$$

Routing in Equilibrium, João Luís Sobrinho and Timothy G. Griffin, MTNS 2010.

Dijkstra's algorithm

Input : adjacency matrix $\mathbf{A}$ and source vertex $i \in V$,
Output : the i-th row of $\mathbf{R}$, $\mathbf{R}(i, \_)$.

begin
  $S \leftarrow \{i\}$
  $\mathbf{R}(i, i) \leftarrow \overline{1}$
  for each $q \in V - \{i\}$: $\mathbf{R}(i, q) \leftarrow \mathbf{A}(i, q)$
  while $S \neq V$
    begin
      find $q \in V - S$ such that $\mathbf{R}(i, q)$ is $\leqslant^{L}_{\oplus}$ -minimal
      $S \leftarrow S \cup \{q\}$
      for each $j \in V - S$
        $\mathbf{R}(i, j) \leftarrow \mathbf{R}(i, j) \oplus (\mathbf{R}(i, q) \otimes \mathbf{A}(q, j))$
    end
end

Classical proofs of Dijkstra's algorithm (for global optimality) assume

Semiring Axioms

$$
\begin{array}{rcrcl}
\mathbb{AS}(\oplus) & : & a \oplus (b \oplus c) & = & (a \oplus b) \oplus c \\
\mathbb{CM}(\oplus) & : & a \oplus b & = & b \oplus a \\
\mathbb{ID}(\oplus) & : & \overline{0} \oplus a & = & a \\
\mathbb{AS}(\otimes) & : & a \otimes (b \otimes c) & = & (a \otimes b) \otimes c \\
\mathbb{IDL}(\otimes) & : & \overline{1} \otimes a & = & a \\
\mathbb{IDR}(\otimes) & : & a \otimes \overline{1} & = & a \\
\mathbb{ANL}(\otimes) & : & \overline{0} \otimes a & = & \overline{0} \\
\mathbb{ANR}(\otimes) & : & a \otimes \overline{0} & = & \overline{0} \\
\mathbb{LD} & : & a \otimes (b \oplus c) & = & (a \otimes b) \oplus (a \otimes c) \\
\mathbb{RD} & : & (a \oplus b) \otimes c & = & (a \otimes c) \oplus (b \otimes c)
\end{array}
$$

Classical proofs of Dijkstra's algorithm assume

Additional axioms

$$\begin{array}{lcccc} \mathbb{SL}(\oplus) & : & a \oplus b & \in & \{a, \; b\} \\ \mathbb{AN}(\oplus) & : & \overline{1} \oplus a & = & \overline{1} \end{array}$$

Note that we can derive right absorption,

$$\mathbb{RA} \quad : \quad a \oplus (a \otimes b) \quad = \quad a$$

and this gives (right) inflationarity, $\forall a, b : a \leqslant a \otimes b$.

$$\begin{array}{rcl} a \oplus (a \otimes b) & = & (a \otimes \overline{1}) \oplus (a \otimes b) \\ & = & a \otimes (\overline{1} \oplus b) \\ & = & a \otimes \overline{1} \\ & = & a \end{array}$$

What will we assume? Very little!

~~Semiring~~ Axioms

$$
\begin{array}{rcrcl}
\mathbb{AS}(\oplus) & : & a \oplus (b \oplus c) & = & (a \oplus b) \oplus c \\
\mathbb{CM}(\oplus) & : & a \oplus b & = & b \oplus a \\
\mathbb{ID}(\oplus) & : & \overline{0} \oplus a & = & a \\
\cancel{\mathbb{AS}(\otimes)} & : & \cancel{a \otimes (b \otimes c)} & \cancel{=} & \cancel{(a \otimes b) \otimes c} \\
\mathbb{IDL}(\otimes) & : & \overline{1} \otimes a & = & a \\
\cancel{\mathbb{IDR}(\otimes)} & : & \cancel{a \otimes \overline{1}} & \cancel{=} & \cancel{a} \\
\cancel{\mathbb{ANL}(\otimes)} & : & \cancel{\overline{0} \otimes a} & \cancel{=} & \cancel{\overline{0}} \\
\cancel{\mathbb{ANR}(\otimes)} & : & \cancel{a \otimes \overline{0}} & \cancel{=} & \cancel{\overline{0}} \\
\cancel{\mathbb{LD}} & : & \cancel{a \otimes (b \oplus c)} & \cancel{=} & \cancel{(a \otimes b) \oplus (a \otimes c)} \\
\cancel{\mathbb{RD}} & : & \cancel{(a \oplus b) \otimes c} & \cancel{=} & \cancel{(a \otimes c) \oplus (b \otimes c)}
\end{array}
$$

What will we assume?

Additional axioms

$$\begin{array}{rcrcl} \mathbb{SL}(\oplus) & : & a \oplus b & \in & \{a,\ b\} \\ \mathbb{ANL}(\oplus) & : & \overline{1} \oplus a & = & \overline{1} \\ \mathbb{RA} & : & a \oplus (a \otimes b) & = & a \end{array}$$

- Note that we can no longer derive $\mathbb{RA}$, so we must assume it.
- Again, $\mathbb{RA}$ says that $a \leqslant a \otimes b$.
- We don't use $\mathbb{SL}$ explicitly in the proofs, but it is implicit in the algorithm's definition of q_k.
- We do not use $\mathbb{AS}(\oplus)$ and $\mathbb{CM}(\oplus)$ explicitly, but these assumptions are implicit in the use of the "big-$\oplus$" notation.

Under these weaker assumptions ...

Theorem (Sobrinho/Griffin)

Given adjacency matrix $\mathbf{A}$ and source vertex $i \in V$, Dijkstra's algorithm will compute $\mathbf{R}(i, \_)$ such that

$$\forall j \in V : \mathbf{R}(i, j) = \mathbf{I}(i,j) \oplus \bigoplus_{q \in V} \mathbf{R}(i, q) \otimes \mathbf{A}(q, j).$$

That is, it computes one row of the solution for the right equation

$$\mathbf{R} = \mathbf{RA} \oplus \mathbf{I}.$$

Dijkstra's algorithm, annotated version

Subscripts make proofs by induction easier ....

begin
  $S_1 \leftarrow \{i\}$
  $\mathbf{R}_1(i,\ i) \leftarrow \overline{1}$
  for each $q \in V - S_1$: $\mathbf{R}_1(i,\ q) \leftarrow \mathbf{A}(i,\ q)$
  for each $k = 2,\ 3,\ \ldots,\ \mid V \mid$
    begin
      find $q_k \in V - S_{k-1}$ such that $\mathbf{R}_{k-1}(i,\ q_k)$ is $\leqslant_{\oplus}^{L}$ -minimal
      $S_k \leftarrow S_{k-1} \cup \{q_k\}$
      for each $j \in V - S_k$
        $\mathbf{R}_k(i,\ j) \leftarrow \mathbf{R}_{k-1}(i,\ j) \oplus (\mathbf{R}_{k-1}(i,\ q_k) \otimes \mathbf{A}(q_k,\ j))$
    end
end

Main Claim, annotated

$$\forall k : 1 \leqslant k \leqslant\mid V \mid \Longrightarrow \forall j \in S_k : \mathbf{R}_k(i,\ j) = \mathbf{I}(i,j) \oplus \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ j)$$

We will use

Observation 1 (no backtracking) :

$$\forall k : 1 \leqslant k <\mid V \mid \Longrightarrow \forall j \in S_{k+1} : \mathbf{R}_{k+1}(i,\ j) = \mathbf{R}_k(i,\ j)$$

Observation 2 (Dijkstra is “greedy”):

$$\forall k : 1 \leqslant k \leqslant\mid V \mid \Longrightarrow \forall q \in S_k : \forall w \in V - S_k : \mathbf{R}_k(i,\ q) \leqslant \mathbf{R}_k(i,\ w)$$

Observation 3 (Accurate estimates):

$$\forall k : 1 \leqslant k \leqslant\mid V \mid \Longrightarrow \forall w \in V - S_k : \mathbf{R}_k(i,\ w) = \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ w)$$

Observation 1

$$\forall k : 1 \leqslant k <\mid V \mid \implies \forall j \in S_{k+1} : \mathbf{R}_{k+1}(i,\ j) = \mathbf{R}_k(i,\ j)$$

Proof: This is easy to see by inspection of the algorithm. Once a node is put into S its weight never changes again.

The algorithm is "greedy"

Observation 2

$$\forall k : 1 \leqslant k \leqslant \mid V \mid \implies \forall q \in S_k : \forall w \in V - S_k : \mathbf{R}_k(i,\ q) \leqslant \mathbf{R}_k(i,\ w)$$

By induction.
Base : Since $S_1 = \{i\}$ and $\mathbf{R}_1(i,\ i) = \overline{1}$, we need to show that

$$\overline{1} \leqslant \mathbf{A}(i,\ w) \equiv \overline{1} = \overline{1} \oplus \mathbf{A}(i,\ w).$$

This follows from $\mathbb{ANL}(\oplus)$.
Induction: Assume $\forall q \in S_k : \forall w \in V - S_k : \mathbf{R}_k(i,\ q) \leqslant \mathbf{R}_k(i,\ w)$ and show $\forall q \in S_{k+1} : \forall w \in V - S_{k+1} : \mathbf{R}_{k+1}(i,\ q) \leqslant \mathbf{R}_{k+1}(i,\ w)$.
Since $S_{k+1} = S_k \cup \{q_{k+1}\}$, this means showing

$$\begin{array}{ll} (1) & \forall q \in S_k : \forall w \in V - S_{k+1} : \mathbf{R}_{k+1}(i,\ q) \leqslant \mathbf{R}_{k+1}(i,\ w) \\ (2) & \forall w \in V - S_{k+1} : \mathbf{R}_{k+1}(i,\ q_{k+1}) \leqslant \mathbf{R}_{k+1}(i,\ w) \end{array}$$

By Observation 1, showing (1) is the same as

$$\forall q \in S_k : \forall w \in V - S_{k+1} : \mathbf{R}_k(i,\ q) \leqslant \mathbf{R}_{k+1}(i,\ w)$$

which expands to (by definition of $\mathbf{R}_{k+1}(i,\ w)$)

$$\forall q \in S_k : \forall w \in V - S_{k+1} : \mathbf{R}_k(i,\ q) \leqslant \mathbf{R}_k(i,\ w) \oplus (\mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ w))$$

But $\mathbf{R}_k(i,\ q) \leqslant \mathbf{R}_k(i,\ w)$ by the induction hypothesis, and $\mathbf{R}_k(i,\ q) \leqslant (\mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ w))$ by the induction hypothesis and $\mathbb{RA}$.
Since $a \leqslant^L_\oplus b \wedge a \leqslant^L_\oplus c \implies a \leqslant^L_\oplus (b \oplus c)$, we are done.

By Observation 1, showing (2) is the same as showing

$$\forall w \in V - S_{k+1} : \mathbf{R}_k(i,\ q_{k+1}) \leqslant \mathbf{R}_{k+1}(i,\ w)$$

which expands to

$$\forall w \in V - S_{k+1} : \mathbf{R}_k(i,\ q_{k+1}) \leqslant \mathbf{R}_k(i,\ w) \oplus (\mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ w))$$

But $\mathbf{R}_k(i,\ q_{k+1}) \leqslant \mathbf{R}_k(i,\ w)$ since q_{k+1} was chosen to be minimal, and $\mathbf{R}_k(i,\ q_{k+1}) \leqslant (\mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ w))$ by $\mathbb{RA}$.
Since $a \leqslant^L_\oplus b \wedge a \leqslant^L_\oplus c \implies a \leqslant^L_\oplus (b \oplus c)$, we are done.

Observation 3

Observation 3

$$\forall k : 1 \leqslant k \leqslant \mid V \mid \Longrightarrow \forall w \in V - S_k : \mathbf{R}_k(i,\ w) = \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ w)$$

Proof: By induction:

Base : easy, since

$$\bigoplus_{q \in S_1} \mathbf{R}_1(i,\ q) \otimes \mathbf{A}(q,\ w) = \overline{1} \otimes \mathbf{A}(i,\ w) = \mathbf{A}(i,\ w) = \mathbf{R}_1(i,\ w)$$

Induction step. Assume

$$\forall w \in V - S_k : \mathbf{R}_k(i,\ w) = \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ w)$$

and show

$$\forall w \in V - S_{k+1} : \mathbf{R}_{k+1}(i,\ w) = \bigoplus_{q \in S_{k+1}} \mathbf{R}_{k+1}(i,\ q) \otimes \mathbf{A}(q,\ w)$$

By Observation 1, and a bit of rewriting, this means we must show

$$\forall w \in V - S_{k+1} : \mathbf{R}_{k+1}(i,\ w) = \mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ w) \oplus \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q$$

Using the induction hypothesis, this becomes

$$\forall w \in V - S_{k+1} : \mathbf{R}_{k+1}(i,\ w) = \mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ w) \oplus \mathbf{R}_k(i,\ w)$$

But this is exactly how $\mathbf{R}_{k+1}(i,\ w)$ is computed in the algorithm.

Proof of Main Claim

Main Claim

$$\forall k : 1 \leqslant k \leqslant \mid V \mid \Longrightarrow \forall j \in S_k : \mathbf{R}_k(i,\ j) = \mathbf{I}(i,j) \oplus \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ j)$$

Proof : By induction on k.
Base case: $S_1 = \{i\}$ and the claim is easy.
Induction: Assume that

$$\forall j \in S_k : \mathbf{R}_k(i,\ j) = \mathbf{I}(i,j) \oplus \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ j)$$

We must show that

$$\forall j \in S_{k+1} : \mathbf{R}_{k+1}(i,\ j) = \mathbf{I}(i,j) \oplus \bigoplus_{q \in S_{k+1}} \mathbf{R}_{k+1}(i,\ q) \otimes \mathbf{A}(q,\ j)$$

Since $S_{k+1} = S_k \cup \{q_{k+1}\}$, this means we must show

$$\begin{array}{ll} (1) & \forall j \in S_k : \mathbf{R}_{k+1}(i,\ j) = \mathbf{I}(i,j) \oplus \bigoplus_{q \in S_{k+1}} \mathbf{R}_{k+1}(i,\ q) \otimes \mathbf{A}(q,\ j) \\ (2) & \mathbf{R}_{k+1}(i,\ q_{k+1}) = \mathbf{I}(i,q_{k+1}) \oplus \bigoplus_{q \in S_{k+1}} \mathbf{R}_{k+1}(i,\ q) \otimes \mathbf{A}(q,\ q_{k+1}) \end{array}$$

By use Observation 1, showing (1) is the same as showing

$$\forall j \in S_k : \mathbf{R}_k(i,\ j) = \mathbf{I}(i,j) \oplus \bigoplus_{q \in S_{k+1}} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ j),$$

which is equivalent to

$$\forall j \in S_k : \mathbf{R}_k(i,\ j) = \mathbf{I}(i,j) \oplus (\mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ j)) \oplus \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ j$$

By the induction hypothesis, this is equivalent to

$$\forall j \in S_k : \mathbf{R}_k(i,\ j) = \mathbf{R}_k(i,\ j) \oplus (\mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ j)),$$

Put another way,

$$\forall j \in S_k : \mathbf{R}_k(i,\ j) \leqslant \mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ j)$$

By observation 2 we know $\mathbf{R}_k(i,\ j) \leqslant \mathbf{R}_k(i,\ q_{k+1})$, and so

$$\mathbf{R}_k(i,\ j) \leqslant \mathbf{R}_k(i,\ q_{k+1}) \leqslant \mathbf{R}_k(i,\ q_{k+1}) \otimes \mathbf{A}(q_{k+1},\ j)$$

by $\mathbb{RA}$.

To show (2), we use Observation 1 and $\mathbf{I}(i, q_{k+1}) = \overline{0}$ to obtain

$$\mathbf{R}_k(i,\ q_{k+1}) = \bigoplus_{q \in S_{k+1}} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ q_{k+1})$$

which, since $\mathbf{A}(q_{k+1},\ q_{k+1}) = \overline{0}$, is the same as

$$\mathbf{R}_k(i,\ q_{k+1}) = \bigoplus_{q \in S_k} \mathbf{R}_k(i,\ q) \otimes \mathbf{A}(q,\ q_{k+1})$$

This then follows directly from Observation 3.

Finding Left Local Solutions?

$$\mathbf{L} = (\mathbf{A} \otimes \mathbf{L}) \oplus \mathbf{I} \quad \Longleftrightarrow \quad \mathbf{L}^T = (\mathbf{L}^T \otimes^T \mathbf{A}^T) \oplus \mathbf{I}$$

$$\mathbf{R}^T = (\mathbf{A}^T \otimes^T \mathbf{R}^T) \oplus \mathbf{I} \quad \Longleftrightarrow \quad \mathbf{R} = (\mathbf{R} \otimes \mathbf{A}) \oplus \mathbf{I}$$

where

$$a \otimes^T b = b \otimes a$$

Replace $\mathbb{RA}$ with $\mathbb{LA}$,

$$\mathbb{LA} : \forall a, b : a \leqslant b \otimes a$$